

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for managing the use of electronic content at a user's computing device, the method including:

executing an application program on the user's computing device, the application program being capable of rendering electronic content, the application program having at least a first digital certificate associated therewith;

requesting the application program to render a piece of electronic content, the piece of electronic content having at least a second digital certificate associated therewith, and the piece of electronic content further having associated therewith at least one electronic rule, the at least one electronic rule including data specifying one or more conditions associated with rendering the piece of electronic content, the one or more conditions including a condition that the piece of electronic content may be rendered by an application program having the first digital certificate associated therewith;

verifying the association of the second digital certificate with the piece of electronic content;

using a rights management program running on the user's computing device to examining the data included in the at least one electronic rule and to determine that the piece of electronic content may be rendered by an application program having the first digital certificate associated therewith;

verifying the association of the first digital certificate with the application program

using the rights management program; and

rendering the piece of electronic content using the application program.

2. (Previously Presented) A method as in claim 1, in which the first digital certificate is generated by a first entity, and the second digital certificate is generated by a second entity different from the first entity.
3. (Previously Presented) A method as in claim 2, in which the first entity comprises an association of one or more content providers, and the first digital certificate is associated with the application program if the application program meets certain predefined criteria set by the association.
4. (Previously Presented) A method as in claim 3, in which the second entity comprises an entity concerned with controlling the nature of the electronic content that is rendered by the application program, and the second digital certificate is associated with the piece of electronic content if the piece of electronic content meets certain predefined standards.
5. (Previously Presented) A method as in claim 4, in which the second entity comprises a private or governmental entity that determines whether content is appropriate for minors, and the second digital certificate indicates that the piece of electronic content is deemed to be appropriate for minors.
6. (Previously Presented) A method as in claim 3, in which the piece of electronic content comprises a prescription, and in which the first entity associates the first digital

certificate with the application program if it is determined that the application program will handle the prescription with at least a predefined level of security.

7. (Original) A method as in claim 6, in which the predefined level of security includes a requirement that the application verify that an application user has a predefined certificate before rendering the prescription.

8. (Currently Amended) A method as in claim 7, in which predefined certificate indicates that the application user is a licensed pharmacist.

9. (Previously Presented) A method as in claim 7, in which a certified pharmacist is identified by a digital certificate issued by a third entity different from the first and second entities.

10. (Previously Presented) A method as in claim 4, in which the second entity associates the second digital certificate with the prescription if the prescription originated from a certified physician.

11. (Currently Amended) A method as in claim 10, in which a certified physician is identified by a third digital certificate issued by a third entity different from the first and second entities.

12. (Currently Amended) A method as in claim 11, in which the second entity determines that a prescription originated from a certified physician by checking for the presence of the third digital certificate issued by the third entity.

13. (Currently Amended) A method as in claim 12, in which the ~~rendering~~ application program is further associated with a fourth digital certificate, the fourth digital certificate attesting to a determination having been made by a fourth entity that the application program possesses a predefined functionality.

14. (Previously Presented) A method as in claim 13, in which the predefined functionality includes functionality that ensures that the application program verifies the association of the second digital certificate with the piece of electronic content before rendering the piece of electronic content.

15. (Previously Presented) A method as in claim 14, further including:

verifying the association between the application and the fourth digital certificate.

16. (Previously Presented) A method as in claim 1, in which the step of verifying the association of the second digital certificate with the piece of electronic content is performed during or after the step of verifying the association of the first digital certificate with the application program.

17. (Currently Amended) A method as in claim 1, in which the step of verifying the association of the first digital certificate with the application program includes computing a hash of at least part of the application program[[.]] and comparing the hash to a value contained in the digital certificate.

18. (Currently Amended) A method as in claim 1, further including:

decrypting a secure container containing the piece of electronic content and the at least one electronic rule; and

retrieving the at least one electronic rule from the secure container.

19. (Currently Amended) A method performed by a user's computing device, the method comprising:

receiving, at a rights management program running on the user's computing device, a request from an application program running on the user's computing device to render a piece of electronic content, the piece of electronic content having at least one electronic rule associated therewith, the at least one electronic rule including data specifying one or more conditions associated with rendering the piece of electronic content, the one or more conditions including a condition that the piece of electronic content may be rendered by an application program having a predefined digital certificate associated therewith, the predefined digital certificate attesting to the application program's possession of one or more characteristics;
~~retrieving the electronic rule;~~

~~examining the data included in the electronic rule to determine that the piece of electronic content may be rendered by an application program having the predefined digital certificate associated therewith;~~
using the rights management program to examine the data included in the electronic rule and to verifying the association of the predefined digital certificate with the application program in accordance with the electronic rule; and
~~granting the request to rendering~~ the piece of electronic content using the application program upon successful verification of the association of the predefined digital certificate with the application program if the verifying step is successful.

20. (Currently Amended) A method as in claim 19, in which the predefined digital certificate indicates that the application program is operable to check[[s]] output drivers for integrity.